



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,788	06/29/2001	Thomas L. Stachura	42390P10773	5580

8791 7590 10/02/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER

SHIFERAW, ELEN I A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 10/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/895,788		STACHURA ET AL.	
	Examiner		Art Unit	
	Eleni A. Shiferaw		2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 July 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5,7,8,10-12,14-17,19-21,23-28 and 30-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5,7,8,10-12,14-17,19-21,23-28 and 30-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments with respect to amended claims 1, 3, 4, 17, 31, 32, 36, and 37, and currently pending claims 1-5, 7, 8, 10-12, 14-17, 19-21, 23-28, and 30-37 filed on 07/17/2006 have been fully considered but they are not persuasive and some arguments are moot in view of new ground of rejections.

Response to Arguments

The Applicant's first argument concerns Jari failure to disclose "*a plurality of synchronized security sequence values*" as recited in claims 1, 5, 14, 17, 20, 28, 31, and 33 (remark page 13 lines 6-7). The examiner respectfully disagrees with the Applicant's contentions and would like to draw the Applicant's attention to reference Jari where he discloses an IP security-capable security gateway comprising **security association database** for controlling secure communications between the network and external users (see, abstract) and the security gateway retrieves the most recently stored security association number during loss of communication with external user **in the event of power failure or any other failure** and provides/injects the retrieved **security association number to resynchronize the communication** (see 0037) or calculates and injects the correct security association number to resynchronize communication between the security gateway and external user (see, 0038-0040).

The Applicant's argument concerns Jari failure to disclose "*the detection of an event desynchronizing the secured communications*" as recited in claims 1, 5, 14, 17, 20, 28, 31, and 33 (remark page 13 lines 7-8). The examiner respectfully disagrees with the Applicant's contentions and would like to draw the Applicant's attention to par. 0037, and 0034 where in Jari

discloses detecting power failure or possible certain other/any failure that causes the secure communications between secure gateway and external user to be desynchronized.

Regarding arguments “receiving a second resynchronization value in a response to the first resynchronization value” or for “reestablishing secured communication using the first resynchronization value and second resynchronization value” reference Johnson is combined see detailed office action below.

The applicant’s argument concerns Gambino and Johnson failure to disclose, “... sequence values or authentication of secure communications or synchronized security values” as recited in claims 1, 5, 14, 17, 20, 28, 31, and 33 (remark page 15 lines 14-17, page 16 lines 5-9, and page 17 lines 10-12). The examiner respectfully disagrees with the applicant’s contentions and would like to draw the Applicant’s attention to col. 1 line 21-col. 2 lines 56 wherein Gambino discloses the invention is to the recovery of network operations after a failure of a network unit that causes loss of data messages sent on an RTP connection in the network, and out of order arrival of data messages. Each data message contains a SYNC number and a byte sequence number (BSN) that enables the destination node to determine when data is lost or arrives out of order. A recipient of each message tests to determine whether the message has a **next expected byte sequence number** and discards any BSN older than the next expected byte sequence number. The system includes means for retrieving, after the failure of the data processor unit, a stored SYNC number and BSN, means for incrementing the SYNC number and BSN by a predetermined amount to obtain a new SYNC number to insure that the new SYNC number comprises a current SYNC number, means for sending a message from the first node to a second node and the message including SYNC number and BSN, response message for received

message that contain a BSN of a next piece of data, and when power offs/component failure occurs, resynchronizing the disconnected BSN and SYNC number of the communication for secure communication. It is clear that Gambino does in fact teach secure sequence values for authentication of secure communications as recited in claims 1, 5, 14, 17, 20, 28, 31, and 33. Moreover, Examiner would like to refer to pages 2-4 of Applicant's BACKGROUND of the disclosure wherein "***Network security schemes are not new. Network security schemes may be used to secure a single communication path between two users. An example of a network security schemes is the IP security that provides authenticity/confidentiality guarantees for each data packet sent between network nodes. IP security offers protocol for security schemes such as anti-replay logic using security sequence values, and cryptography key management. Anti-replay logic uses security sequence values to allow communicating devices to ignore data packets that have been previously received. These prevents computing devices that are outside a security connection from stealing confidential data by faking the IP address of another legitimate user on the secure connection and using exact duplicates of wiretapped data packets to fraudulently engage in the secure communication. Various other security implementations that conform to IP security may also utilize security sequence values to prevent spoofing. IP security also mandates support for cryptography key management and authentication algorithms and communications***"

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Applicant's Admitted Prior Art within the system of applied prior art(s) because they are analogous in network communication security when desynchronization occurs. One would have been motivated to do so because it would

resynchronize the communication to allow sender and receiver exchange data messages securely without missing data during desynchronization. Moreover, Johnson discloses security sequence values by sending multicast messages by a sender device wherein the message contains information/security sequence number that allows intended receiver device to check and determine the possibility that earlier-sent multicast messages from the sender node were not received by the receiver node (see abstract). “When a multicast message is received, the receiver node will check the sequence number contained in the message. If the sequence number is out of sequence, the receiver node will queue the message in an ordered queue and then check the queue for the missing least sequence number message, and send a negative acknowledgement for the multicast message corresponding to such missing least sequence number. On the other hand, if the sequence number or the DOB marker contained in the multicast message do not match the sequence number or marker expected by the receiver node, a resynchronization request message will be returned by the receiver node to the sender node. The resynchronization request will cause the sender node to respond with its new marker, and the sequence number of the last multicast message unacknowledged by the receiving node. In this way, lost multicast messages can be accounted for and delivered.” (see col. 2 lines 44-60). Therefore argument is not persuasive. It is clear that both Gambino and Johnson do disclose the teachings of “security sequence values” or “authentication of secure communications” or “synchronized security values” as claimed.

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-4, 31-32, and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by Gambino (Patent No.: US 6,339,796 B1).

As per claim 1 and 31, Gambino discloses a method comprising:

establishing secured communication between a client device and server device; wherein communication is secured using, at least in part, synchronized security sequence value(s) for authentication of secure communications (col. 3 lines 32-37 and lines 55-59, and col. 7 lines 13-21; *data host/first data processing system (12) and remote system/second data processing system (16) are synchronized using sequence numbers*);

storing a security sequence value as a resynchronization value (col. 4 lines 24-41; *periodically storing/refreshing sequence numbers for recovery of system failure and/or for resynchronization request*);

detecting at least one event desynchronizing said secured communication (col. 4 lines 34-37 and claim 1 lines 6-20; *de-synchronization/failure of data host is detected*); and

requesting resynchronization of security sequence values, comprising sending at least a representation of said first resynchronization value from said client device to said server device

(col. 2 lines 33-37, col. 5 lines 1-5, and claim 1 lines 26-29; *data host (12) sending status request message packet/resynchronization request that includes sequence number stored on external device of the data host (12)*).

“receiving a second resynchronization value in a response to the first resynchronization value; and reestablishing secure communication using the first resynchronization value and the second resynchronization value”, as amended (col. 2 lines 33-56 and claim 1 lines 30-34; *first data processing system sending status request to second data processing system during de-synchronization/failure of host, wherein the status request containing new SYNC number and last BSN read from the memory and receiving a response message from second data processing system for re-synchronizing communication, response message containing next BSN sequence number that the first data processing system is expecting*).

As per claim 2, Gambino teaches the method, further comprising performing anti-replay filtering using said security sequence values (col. 4 lines 54-58; *discarding duplicate sequence numbers...*).

As per claim 3, Gambino teaches the method, wherein sending at least a representation of said first resynchronization value includes embedding said first resynchronization value in at least one header and/or at least one payload of a data packet (col. 4 lines 45-50; *a header transport/THDR containing sequence number...*).

As per claims 4 and 32, Gambino teaches the method/medium, wherein said storing a client

resynchronization value includes periodically refreshing a stored first resynchronization value with a new value at a selected interval from security sequence values already used in a secured communication session (col. 4 lines 24-41 and col. lines 33-55).

As per claim 39, Gambino teaches the method, further comprising resynchronizing the secured communication using the resynchronization value and the second resynchronization value (claim 13 lines 47-col. 12 lines 12; *the resynchronization value sent from data host (12) and resynchronization value replied from remote system is used for resynchronization*).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 5, 7-8, 10-12, 14-17, 19-21, 23-28, 30, 33-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gambino (Patent No.: US 6,339,796 B1) in view of Johnson et al. (Johnson, Patent No.: US 6,247,059 B1).

As per claim 5, Gambino discloses the method comprising:

establishing secured communication between a client device and server device; wherein communication is secured using, at least in part, a plurality of synchronized security sequence values for authentication of secure communication (col. 3 lines 32-37 and lines 55-59, and col. 7

lines 13-21; *data host/first data processing system (12) and remote system/second data processing system (16) are synchronized using sequence numbers*);

receiving a request for resynchronization from the client device, the request including at least a representation of a client resynchronization value, the client resynchronization value being a stored synchronized security value of the plurality of synchronized security sequence values (col. 2 lines 33-46, col. 5 lines 5-7 and col. 4 lines 24-41; *remote device (16) receives the resynchronization request from data host (12), wherein the request message includes sequence number/resynchronization value that is stored on external memory of data host for resynchronization*);

acknowledging the client request for resynchronization (col. 2 lines 39-46 and claim 1 lines 30-34; *acknowledgment response including the remote system resynchronization value is sent to data host to reestablish communication*); and

reestablishing secured communication using said client resynchronization value and said server resynchronization value (claim 1 lines 35-38, and col. 6 lines 37-46; *communication is reestablished*).

Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value. Gambino does not explicitly teach that the replay message including resynchronization value sent from data host.

However Johnson discloses an acknowledging comprising sending the representation of resynchronization value and at least a representation of a server resynchronization value from said server device to said client device (Johnson col. 2 lines 18-60; *establishing communication*

*and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its **new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value**).*

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claim 14, Gambino discloses an apparatus, comprising;

(a) a security interface to engage in secured communication with at least one network node, wherein said security interface and said at least one network node use synchronized security sequence values at least in part to authenticate said secured communication (col. 3 lines 32-37 and lines 55-59, and col. 7 lines 13-21; *data host/first data processing system (12) and remote system/second data processing system (16) are synchronized using sequence numbers*);

(i) a recorder to store at least one security sequence value (col. 4 lines 24-41; *periodically storing/refreshing sequence numbers for recovery of system failure and/or for resynchronization request*);

(ii) a desynchronization detector coupled to said security interface (col. 4 lines 34-37 and claim 1 lines 6-20; *de-synchronization/failure of data host is detected by detector of data host (12)*);

(iii) a resynchronization requester to send the stored security sequence value to at least one network node after a desynchronization (col. 2 lines 33-37, col. 5 lines 1-5, and claim 1 lines 26-29; *data host (12) sending status request message packet/resynchronization request that includes sequence number stored on external device of the data host (12)*); and

(iv) a verifier to receive feedback from said at least one network node (claim 13 lines 47-col. 12 lines 12);

(b) a security agent coupled to said at least one network node, comprising:

(i) a request receiver to recognize said stored security sequence value (col. 7 lines 52-65; *remote system, that recognizes the stored sequence values, receives the resynchronization request sent from data host (12) and replies to the request for resynchronization*); and

(ii) an acknowledger to send said feedback from said security agent to said security interface; said feedback comprising a node security sequence value from said network node (col. 2 lines 39-46 and claim 1 lines 30-34; *acknowledgment response including the remote system resynchronization value is sent to data host to reestablish communication from acknowledger remote system*).

Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value. Gambino does not explicitly teach that the replay message including resynchronization value sent from data host.

However Johnson discloses a feedback comprising requester's sequence value (Johnson col. 2 lines 18-60; *establishing communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claim 17, Gambino discloses a computer network security sequence value resynchronizer, comprising:

(a) a sender having at least access to a nonvolatile random access memory (col. 4 lines 24-41; *data host has access to periodically stored sequence numbers for recovery of system failure and/or for resynchronization request*);

(b) said sender to transmit a data packet containing at least in part a stored sender resynchronization value of security sequence values for authentication of secure communications from said nonvolatile random access memory over said computer network (col. 2 lines 33-37, col. 5 lines 1-5, and claim 1 lines 26-29; *data host (12) sending status request message packet/resynchronization request that includes sequence number stored on external device of the data host (12)*); and

(c) an acknowledger connected to said computer network to receive said sender resynchronization value from said sender, the communications to be resynchronized using the sender resynchronization value and the acknowledger resynchronization value (col. 2 lines 39-46, claim 1 lines 30-34, and col. 2 lines 33-56; *acknowledger remote system receives requests and returns acknowledgment response including the remote system resynchronization value*);

Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value. Gambino does not explicitly teach that the replay message including resynchronization value sent from data host.

However Johnson discloses a said acknowledger returning said sender resynchronization value to said sender as security assurance, the communications to be resynchronized using the

sender resynchronization value and the acknowledger resynchronization value (Johnson col. 2 lines 18-60; *establishing communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claim 20, Gambino disclose a method comprising:

establishing secured communication between a security interface and a network node, said security interface to resynchronize security sequence values for authentication of secure communications between said security interface and said network node (col. 3 lines 32-37 and

lines 55-59, and col. 7 lines 13-21; *data host/first data processing system (12) and remote system/second data processing system (16) are synchronized using sequence numbers*);

storing a first resynchronization value selected by said security interface (col. 4 lines 24-41; *periodically storing/refreshing sequence numbers for recovery of system failure and/or for resynchronization request*); and

resynchronizing said security sequence values after a break in said secured communication (claim 1 lines 35-38, and col. 6 lines 37-46; *communication is reestablished*), said resynchronizing further comprising:

sending said first resynchronization value from said security interface to said network node (col. 2 lines 33-37, col. 5 lines 1-5, and claim 1 lines 26-29; *data host (12) sending status request message packet/resynchronization request that includes sequence number stored on external device of the data host (12)*);

sending said a second resynchronization value from said network node to said security interface (col. 2 lines 39-46 and claim 1 lines 30-34; *acknowledgment response including the remote system resynchronization value is sent to data host to reestablish communication*); and

reestablishing said secured communication using said first resynchronization value and said second resynchronization value (claim 1 lines 35-38, and col. 6 lines 37-46; *communication is reestablished using the data host resynchronization value sent from data host and resynchronization value received from remote system*).

Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value. Gambino does not explicitly teach sending said first

resynchronization value from said network node to said security interface (the replay message including resynchronization value sent from data host).

However Johnson discloses sending said first resynchronization value from said network node to said security interface (Johnson col. 2 lines 18-60; *establishing communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claim 28, Gambino discloses a method, comprising:

establishing secured communication between a server device and a client device, said secured communication using server security sequence values synchronized with client security sequence values for authentication of secure communications (col. 3 lines 32-37 and lines 55-59, and col. 7 lines 13-21; *data host/first data processing system (12) and remote system/second data processing system (16) are synchronized using sequence numbers*);

storing at least one client security sequence value in nonvolatile memory as a saved client security sequence value (col. 4 lines 24-41; *periodically storing/refreshing sequence numbers for recovery of system failure and/or for resynchronization request*); and

resynchronizing server and client security sequence values after a desynchronization event, resynchronizing including sending said saved client security sequence value from said nonvolatile memory to said server device (col. 2 lines 33-37, col. 5 lines 1-5, and claim 1 lines 26-29; *data host (12) sending status request message packet/resynchronization request that includes sequence number stored on external device of the data host (12)), and returning server security sequence value* (col. 2 lines 39-46 and claim 1 lines 30-34; *response including the remote system/server resynchronization value is sent to data host to reestablish communication*);

Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value. Gambino does not explicitly teach returning said saved client security sequence value from said server device to said client device in a data packet (the replay message including resynchronization value sent from data host).

However Johnson discloses returning said saved client security sequence value from said server device to said client device in a data packet (Johnson col. 2 lines 18-60; *establishing*

communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claim 33, Gambino teaches a machine-readable medium having stored thereon data representing sequences of instructions that, when executed by a processor, cause the processor to perform operations comprising:

establishing secured communication between a client device and server device (col. 3 lines 32-37); wherein communication is secured using, at least in part a plurality of synchronized security sequence values for authentication of secure communications (col. 3 lines

32-37 and lines 55-59, and col. 7 lines 13-21; *data host/first data processing system (12) and remote system/second data processing system (16) are synchronized using sequence numbers*);

receiving a request for resynchronization from the client device, the request including a resynchronization value, the resynchronization value being a stored synchronized security sequence of the plurality of security sequence values (col. 2 lines 33-46, col. 5 lines 5-7 and col. 4 lines 24-41; *remote device (16) receives the resynchronization request from data host (12), wherein the request message includes sequence number/resynchronization value that is stored on external memory of data host for resynchronization*);

acknowledging the client request for resynchronization, acknowledging comprising sending a server resynchronization value from the server device to the client device (col. 2 lines 39-46 and claim 1 lines 30-34; *acknowledgment response including the remote system resynchronization value is sent to data host to reestablish communication*); and

reestablishing secured communication using the client resynchronization value and the server resynchronization value (claim 1 lines 35-38, and col. 6 lines 37-46; *communication is reestablished using the data host resynchronization value sent from data host and resynchronization value received from remote system*).

Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value. Gambino does not explicitly teach acknowledging comprising sending resynchronization value from the server device to the client device (the replay message including resynchronization value sent from data host).

However Johnson discloses acknowledging comprising sending resynchronization value from the server device to the client device (Johnson col. 2 lines 18-60; *establishing communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claim 7, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, wherein sending at least a representation of said client and said server resynchronization values includes embedding said client and said server resynchronization values in at least one header and/or at least one payload of a data packet that

Art Unit: 2136

conforms to IPsec standards (col. 4 lines 45-50 and col. 3 lines 60-67; *a header transport/THDR containing sequence number...RTP*).

As per claims 8 and 21, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, further comprising performing said method using a state machine in network circuitry (col. 4 lines 24-41).

As per claim 10, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, further comprising performing anti-replay filtering using said synchronized security sequence values (col. 4 lines 54-58; *discarding duplicate sequence numbers...*).

As per claim 15, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, wherein stored security sequence values and node security sequence values are embedded in at least one header and/or at least one payload of a data packet that conforms to IPsec standards (col. 4 lines 45-50 and col. 3 lines 60-67; *a header transport/THDR containing sequence number...RTP*).

As per claim 16, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the apparatus, wherein said stored security sequence value is periodically refreshed with a value at a selected interval from security sequence values already used in a secured communication session (col. 4 lines 24-41).

As per claim 30, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, said storing further comprising periodically refreshing said saved client security sequence value with a number that is greater in value than client security sequence values that have already been sent to said server device in a communication session (col. 4 lines 24-41).

As per claim 36, Johnson et al. teaches the method, wherein the response further includes the first resynchronization value (col. 2 lines 44-60).

As per claim 37, Johnson et al. teaches the method, wherein the first resynchronization value is contained in payload data of the response (col. 2 lines 44-60).

As per claim 38 Gambino discloses all the subject matter as described above. Gambino reestablishes the communication by sending a replay message, for the resynchronization request, that includes remote system's resynchronization value.

Gambino does not explicitly teach response further includes a second resynchronization value (the replay message including resynchronization value sent from data host).

However Johnson discloses response further includes a second resynchronization value (Johnson col. 2 lines 18-60; *establishing communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization*

request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Gambino because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

As per claims 11, 26, and 34, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the medium, further comprising instructions that, when executed by the processor, cause the processor to perform operations comprising reestablishing secured communication during a low-power state (col. 3 lines 63-65 and claim 7; *data host failure is also low-power state. However applicant is advised to refer to Latka, patent number 5,646,996 on col. 6 lines 50-53 and col. 1 lines 10-14 and lines 56-67. Latka discloses detecting loss of synchronization, between transmitter and receiver of remote system, due to momentary power failure or a low battery condition and reestablishes communication by generating a communication sequence. It would have been obvious to one ordinary skill in the art at the time*

of the invention was made to modify low-power stage within the combination system of Gambino and Johnson because low-power stage causes data host failure/loss of data).

As per claims 12 and 27, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, further comprising reestablishing secured communication while said first device lacks an active operating system and/or lacks an active microprocessor (col. 4 lines 34-37).

As per claim 19, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the resynchronizer, wherein at least one sender and at least one acknowledger are installed on any combination of server and client devices (col. 3 lines 29-32).

As per claim 23, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method further comprising storing said first resynchronization value in a nonvolatile storage medium (col. 4 lines 24-41).

As per claim 24, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method further comprising establishing secured communication using IPsec security standards (col. 4 lines 42-45).

As per claim 25, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses method further comprising resynchronizing said secured

Art Unit: 2136

communication using said first resynchronization value to resynchronize secured data sent from said security interface and using said second resynchronization value to resynchronize secured data sent from said network node (claim 1; *resynchronizing the communication by using data host (12) resynchronization value sent from data host (12) and resynchronization value replied from remote system to data host (12)*).

As per claim 35, Gambino and Johnson disclose all the subject matter as described above. In addition Gambino discloses the method, further comprising reestablishing secured communication while the client device lacks an active operating system, lacks an active microprocessor, or both (claim 12 lines 13-46; *failure of data host/first data processing system and resynchronization of the first and second data processing system...*).

6. Claims 1, 5, 14, 17, 20, 28, 31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jari et al. Pub. No.: US 2001/0020275 A1 in view of Johnson et al. (Johnson, Patent No.: US 6,247,059 B1).

As per claims 1, 5, 14, 17, 20, 28, 31, and 33, Jari discloses a method/apparatus/medium comprising:

establishing secured communication between a client device and server device, wherein communication is secured using, at least in part, synchronized security sequence value(s) for authentication of secure communications (see, abstract and 0032; *establishing secure*

communications between the network and external users...using security association database that contains security sequence values for communication authentication);

storing a security sequence value as a resynchronization value (0012-0013, 0015, 0025, 0035 and 0017; *stored security sequence numbers for resynchronization*);

detecting at least one event desynchronizing said secured communication (0034, 0017, and 0020; *detecting temporary failure of communication node*);

requesting resynchronization of security sequence values, comprising sending at least a representation of said resynchronization value from said client device to said server device (0037-0041); and

reestablishing secured communication using said client resynchronization value and said server resynchronization value (claim 1).

Jari discloses all the subject matter as described above. Jari discloses an IP security-capable security gateway comprising security association database for controlling secure communications between the network and external users (see, abstract) and the security gateway retrieves the most recently stored security association number during loss of communication with external user in the event of power failure or any other failure and provides/injects the retrieved security association number to resynchronize the communication (see 0037) or calculates and injects the correct security association number to resynchronize communication between the security gateway and external user (see, 0038-0040). Jari fails to explicitly disclose the requests and responses between the devices, wherein request including first resynchronization value and reestablishing secure communication using first and second resynchronization value.

However, Johnson discloses “receiving a second resynchronization value in a response to the first resynchronization value; and reestablishing secured communication using the first resynchronization value and the second resynchronization value” (Johnson col. 2 lines 18-60; *establishing communication and exchanging multicast message between sender node and receiver node. The multicast message is structured to include a sequence number. When a node fails or sequence number is out of order a resynchronization request is sent from receiver node to sender node and the sender node acknowledges by sending its new marker/server resynchronization value and the sequence number of the last multicast message unacknowledged by the receiving node/negative acknowledgment multicast messages, messages receiver node has not received, sent from receiver node/resynchronization value*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnson within the system of Jari because they are analogous in multi-computer synchronization and re-synchronization method. One would have been motivated to incorporate resynchronization value of the requester along with resynchronization value of the server on acknowledgment/replay message for resynchronization request received because it is well known in the art to include the requester resynchronization value. And also it would verify that the receiver is the right device that the requester intended to be resynchronized with.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sydon et al. Patent NO.: US 6,466,800 B1 for resynchronizing, when desynchronization occurs, in using sequence values stored on nonvolatile memory/RAM, and

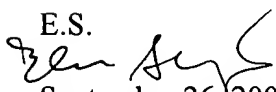
Jung Pub. No.: US 2001/0052072 A1, for resynchronizing communications that is out of synchronization in using sequence number and IP security.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

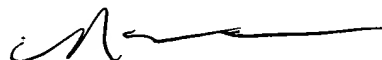
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.


September 26, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


9/27/06